Atty. Dkt. No. 035451-0170 (3708.palm.us.org)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kammer et. al.
Title:	LOCATION BASED SECURITY MODIFICATION SYSTEM AND METHOD
Appl. No.:	10/053,013
Filing Date:	1/18/2002
Examiner:	Abedin, Shanto
Art Unit:	2436
Confirmation No.:	2103

Mail Stop **AMENDMENT**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

STATEMENT OF SUBSTANCE OF INTERVIEW

On June 4, 2009, a telephonic interview took place between Examiner Abedin and counsel of record Steve Becker. Examiner Abedin recommended some additional amendments to the independent claims. No demonstration was conducted or exhibit shown. While no specific agreement as to allowance was reached, Examiner Abedin requested an informal amendment proposal which was submitted (attached hereto).

Respectfully submitted,

Date /July 2, 2009/

FOLEY & LARDNER LLP
Customer Number: 26371
Telephone: (414) 297-5571
Facsimile: (414) 297-4900

By /Steven C. Becker/
    Steven C. Becker
    Attorney for Applicant
    Registration No. 42,308

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Kammer et. al.
Title:	LOCATION BASED SECURITY MODIFICATION SYSTEM AND METHOD
Appl. No.:	10/053,013
Filing Date:	1/18/2002
Examiner:	Abedin, Shanto
Art Unit:	2436
Confirmation No.:	2103

INFORMAL AMENDMENT PROPOSAL

Examiner Abedin: Per our telephone call today, please consider the attached informal amendment proposal.

Thank you,

Steven C. Becker

Reg. No. 42,308

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

     1.   (Currently Amended) A method of adjusting security for a network user node in wireless communication with a network based upon the location of the node, comprising:

          storing a table comprising a plurality of security settings indexed by location in the memory of the network user node;

          determining the location of a network user node;

          selecting a single level of security from the plurality of security ~~levels~~ settings stored in the table based on the determined location, wherein at least one of the plurality of security levels is a default security ~~level~~ setting selected based at least on a determination that the table does not have a location corresponding to the determined location or based at least on the location of the network user node being unknown; and

          modifying a security protection for the network user node based upon the selected level of security setting, wherein the step of modifying the security protection for the network user node includes modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted,

          wherein the determined location and the security protection for the network user node are updated repeatedly.

     18.   (Currently Amended) A computer system for modifying security settings for wireless communications with a network user node based on the location of the node comprising:

          an input device having a communicative coupling with a system for determining the location of a network user node;

          a storage device for storing a table of security modifications to be performed based on a plurality of locations for the network user node, the security modifications including a plurality of levels, the security modifications being defined by a user of the network user node;

-3-

Atty. Dkt. No. 035451-0170 (3708.palm.us.org)

a processor configured to select a data encryption parameter based on the location and the table of security modifications to change whether wireless data transmitted by the computer system to the user node will be encrypted, <u>wherein the processor is configured to select a default security setting if the location is not determined</u>; and

a communication device capable of transmitting a data signal to the network user node based on the selected data encryption parameter;

wherein the location of the network user node and the security protection for the network user node are updated repeatedly.

30.   (Currently Amended) A method of adjusting security for a network user node having a processor, a memory coupled to the processor, a wireless transceiver, and a physical location determining device, wherein the network user node is in communication with a network based upon the physical location of the node, comprising:

storing a table comprising selectable encryption levels indexed by location for each of a plurality of locations in the memory of the network user node;

receiving physical location information using a network user node;

using the network user node to set security protection for wireless data communication to a default encryption level based at least on a determination that the table does not have a location corresponding to the received physical location or based at least on the location of the network user node being unknown; and

using a network user node to modify security protection for wireless data communication to an encryption level selected from the selectable encryption levels, based upon the physical location information;

wherein the table is configurable by a user of the network user node; and

wherein the physical location information and the security protection for the network user node are updated repeatedly.

38. (Currently Amended) A system implemented on a network user node for modifying security settings based on the physical location of the node comprising:

a system for determining the physical location of the network user node coupled to the network user node;

a processor for processing information, storing information on a storage device, and accessing a table of security modifications, the table configured to store security modifications for more than two physical locations; and

a storage device for storing the table of security modifications;

wherein the network user node performs security modifications based on the physical location of the network user node, wherein the security modifications comprise

modifying a data encryption parameter to change whether wireless data transmitted by the network user node will be encrypted, wherein a default security setting is selected based at least on a determination that the table does not have a location corresponding to the received physical location or based at least on the location of the network user node being unknown; and

wherein the physical location and the performance of security modifications for the network user node are updated repeatedly.